Deutscher Bundestag **Drucksache 19/14058**

19. Wahlperiode 16.10.2019

Antrag

der Abgeordneten Konstantin Kuhle, Stephan Thomae, Grigorios Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Dr. Marco Buschmann, Britta Katharina Dassler, Bijan Djir-Sarai, Dr. Marcus Faber, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Manuel Höferlin, Reinhard Houben, Olaf in der Beek, Gyde Jensen, Dr. Christian Jung, Karsten Klein, Dr. Marcel Klinge, Daniela Kluckert, Pascal Kober, Carina Konrad, Konstantin Kuhle, Alexander Graf Lambsdorff, Michael Georg Link, Alexander Müller, Roman Müller-Böhm, Dr. Martin Neumann, Hagen Reinhold, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Frank Sitta, Judith Skudelny, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Michael Theurer, Manfred Todtenhausen, Dr. Andrew Ullmann, Johannes Vogel (Olpe), Nicole Westig, Katharina Willkomm und der Fraktion der FDP

Smart Germany – Digitalisierung und Bürgerrechte

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

1. Vernetzte informationstechnische Systeme wie Smartphones, Assistenzsysteme wie Alexa oder intelligente Alltagsgegenstände gehören heute zum Leben der Menschen und sind ständig und überall präsent. Durch diesen technischen Fortschritt werden Probleme in unterschiedlichen Lebensbereichen gelöst. Es entstehen neue Formen der Kreativität, neue Berufsbilder und neue Räume für wirtschaftliche und persönliche Entfaltung. Menschen rücken näher zusammen, Informationen sind schneller verfügbar, ebenso wie Reaktionen unmittelbarer möglich sind. Es kann nicht Aufgabe der Politik sein, pauschal bestimmte technische Entwicklungen zu untersagen oder Geschäftsmodelle im Vorhinein zu verbieten. Angstmacherei und Abschottung sind die falschen Antworten auf die Herausforderungen der Digitalisierung. Digitale Medienkompetenz und eine verstärkte Vernetzung von Bildung und Digitalisierung ermächtigen den Menschen grundsätzlich, mit den Chancen und Risiken der Digitalisierung frei und eigenverantwortlich umzugehen.
2. Es ist jedoch Aufgabe der Politik, die freie Entfaltung der Persönlichkeit auch unter den Umständen der Digitalisierung umfassend zu schützen. Aufgeschlossenheit und Optimismus mit Blick auf neue digitale Möglichkeiten und Geschäftsmodelle müssen mit einem umfassenden Schutz der Bürgerrechte im Internet einhergehen. Vernetzte informationstechnische System erlauben

es faktisch, einen Menschen rund um die Uhr zu überwachen. Die Bürgerinnen und Bürger werden die Chancen und Vorteile, die mit der Digitalisierung verbunden sind, nur wahrnehmen, wenn sie nicht das Gefühl haben, in einem Netz aus umfassender Überwachung zu leben. Sie müssen darauf vertrauen können, dass die Technik ihrem Willen gehorcht und nicht gegen sie gewandt wird. Dies ist die Essenz des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht“), welches das BVerfG im Jahr 2008 als Ausfluss des Allgemeinen Persönlichkeitsrechts anerkannt hat (BVerfGE 120, 274 Rn. 201 ff.). Damit gilt auch in der digitalen Welt: Die Ausweitung von Kommunikations-, Interaktions- und Überwachungsmöglichkeiten muss stets mit der Möglichkeit verbunden sein, über einen Raum des Rückzugs und der Freiheit vor jeglicher Ausforschung zu verfügen.

3. Viele Menschen möchten vernetzte informationstechnische Systeme, die von privaten Unternehmen angeboten werden, auf der Grundlage einer freien Entscheidung nutzen. So sehr die Politik diesen freien Entschluss zu respektieren hat, so sehr muss sie beim allgemeinen Niveau des Schutzes der Persönlichkeitsentfaltung achtsam sein. Wenn durch die Nutzung vernetzter informationstechnischer Systeme die Daten Dritter unberechtigterweise verarbeitet werden, wenn für Menschen nicht mehr transparent und nachvollziehbar ist, wie ihre Daten genutzt und geschützt werden, oder wenn die Datennutzung über das ursprünglich vereinbarte Maß hinaus geht, muss der Staat einschreiten.

4. Durch grenzenlose Überwachungsmöglichkeiten verfügt auch der Staat selbst potenziell über eine grenzenlose Menge an Daten, auf die er unter bestimmten gesetzlichen Voraussetzungen zugreifen kann. Diese Voraussetzungen brauchen rechtsstaatliche und verlässliche Grenzen. Anderenfalls droht, „ein diffus bedrohliches Gefühl des Beobachtetseins“ (BVerfGE 125, 260 Rn. 212), welches die Wahrnehmung vieler Grundrechte und die Entfaltung der Persönlichkeit sowie der für eine Demokratie essentiellen freien Meinungsbildung empfindlich beeinträchtigen kann. Das Bundesverfassungsgericht hat im Urteil zur Vorratsdatenspeicherung den Gesetzgeber nicht nur größter Zurückhaltung bei der Schaffung neuer Speicherpflichten ermahnt und vor dem Risiko einer totalen Erfassung eines Menschen für seine Freiheitwahrnehmung gewarnt, sondern auch verpflichtet, zuvor eine Gesamtschau der staatlichen Überwachungsmaßnahmen durchzuführen (BVerfGE 125, 260 Rn. 218). Denn eine Überwachungsmaßnahme ist stets nicht nur anhand ihrer eigenen Intensität, sondern immer auch vor dem Hintergrund der übrigen bereits bestehenden Überwachungsmöglichkeiten zu bewerten. Die Summe an Überwachung darf das für die freiheitlich-demokratische Grundordnung erträgliche Maß nicht überschreiten. Eine solche “Überwachungs-Gesamtschau” oder „Überwachungs-Gesamtrechnung“ ist aufgrund der Zunahme der Überwachungsmöglichkeiten dringender denn je.

5. Eine Überwachungs-Gesamtrechnung ist auch deshalb erforderlich, weil in der politischen Diskussion die erforderliche Sensibilität für die Folgen von Überwachungsmaßnahmen und den Wert von Freiräumen für die Bürgerinnen und Bürger fehlt. Dies trat zuletzt wieder zutage, als der Mordfall Lübcke genutzt wurde, um die Aufweitung der Befugnisse des Bundesamtes für Verfassungsschutz voranzutreiben – obwohl das tragische Attentat hierfür keinerlei Anlass gab. Statt reflexhaft die staatlichen Zugriffsmöglichkeiten auszuweiten, sollten endlich die Lehren aus dem NSU-Komplex und dem Attentat am Berliner Breitscheidplatz gezogen werden und eine organisatorische

Neuordnung der Zuständigkeiten und Verantwortlichkeiten erfolgen, die insbesondere das Nebeneinander von siebzehn Verfassungsschutzbehörden beendet.

6. Nach Ansicht der Bundesregierung erlauben die bereits bestehenden Rechtsgrundlagen, insbesondere nach der Strafprozessordnung, den Zugriff auf die verschiedenen Daten, die heute durch vernetzte Geräte gesammelt werden (etwa im Wege einer Beschlagnahme bei einem privaten Unternehmen, das diese Daten sammelt, siehe hierzu die Antwort der Bundesregierung auf die Kleine Anfrage der FDP-Fraktion, Wanzen im Wohnzimmer – Überwachung durch Sprachassistenten und smarte Geräte, Bundestags-Drucksache 19/11478). Es ist zweifelhaft, ob diese – teilweise Jahrzehnte alten – Rechtsgrundlagen, der erhöhten Eingriffstiefe gerecht werden, die durch die Zunahme der Überwachungsmöglichkeiten besteht.

7. Das Vertrauen der Bürgerinnen und Bürger in IT-Systeme setzt voraus, dass diese sicher sind. Die IT-Sicherheit ist die Achillesferse der Informationsgesellschaft. Daher ist der IT-Sicherheit im staatlichen Handeln höchste Priorität einzuräumen (siehe Antrag der FDP-Fraktion, Digitalisierung ernst nehmen – IT-Sicherheit stärken, Bundestags-Drucksache 19/7698). Hiermit verträgt es sich nicht, wenn der Staat sich selbst als Hacker betätigt, Sicherheitslücken, die eine Vielzahl von Bürgern und Unternehmen bedrohen, ankauft oder bewusst offenlässt, um sie später einmal für den heimlichen Zugriff auf IT-Systeme nutzen zu können. Die potentiellen Folgen zeigte deutlich das Schadprogramm „WannaCry“ im Jahr 2017, das Schäden in Millionenhöhe verursachte, indem es eine Lücke in verschiedenen Versionen des Betriebssystems Windows ausnutzte, die den US-Sicherheitsbehörden schon seit Jahren bekannt war.

8. Die anlasslose, undifferenzierte Speicherung von Telekommunikationsverbindungsdaten auf Vorrat (sog. „Vorratsdatenspeicherung“) verstößt nach der eindeutigen Rechtsprechung des Europäischen Gerichtshofes gegen die europäischen Grundrechte, u.a. weil sie „geeignet [ist], bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist“ (EuGH, Rs. 203/15 und C-698/15, Rn. 100 – Tele2 Sverige und Watson). Die deutschen Regelungen hätten bereits längst aufgehoben und Alternativen gesucht werden müssen (z.B. das sogenannte „Quick-Freeze“-Verfahren), denn die Vorratsdatenspeicherung war in der Praxis ausgesetzt. Das Bundesverwaltungsgericht hat die deutschen Regelungen nun dem Europäischen Gerichtshof vorgelegt (-BVerwG 6 C 12.18 - Beschluss vom 25. September 2019).

II. Der Deutsche Bundestag fordert die Bundesregierung daher auf,

1. im Rahmen jedes Gesetzesvorhabens, durch welches neue Überwachungsbefugnisse eingeführt werden sollen – wie vom Bundesverfassungsgericht vorgesehen – eine Überwachungsgesamtrechnung durchzuführen, aus der hervorgeht, welche die Auswirkungen der zusätzlichen Überwachungs- und Informationserhebungsmaßnahmen im Zusammenspiel mit bereits bestehenden Befugnissen bewertet, insbesondere ob die Gesamtschau der Befugnisse geeignet ist, ein „diffus bedrohliches Gefühl des Beobachtetseins“ (BVerfGE 125, 260 Rn. 212) zu erzeugen und ob vor dem Hintergrund bestehender und neuer Maßnahmen das für die freiheitlich-demokratische Grundordnung erträgliche Maß überschritten ist; hier ist auch die Informationssammlung durch Private zu berücksichtigen, auf die staatliche Stellen zugreifen können.

2. die bestehenden Rechtsgrundlagen, die einen Zugriff auf vernetzte Geräte (z.B. Assistenzsysteme wie Alexa oder das vernetzte Auto erlauben) zu überprüfen, ob sie angesichts der Zunahme der Überwachungsmöglichkeiten angepasst werden müssen, insbesondere um den verfassungsrechtlichen Grundlagen zu genügen, und dem Deutschen Bundestag bis 30. Juni 2020 hierzu einen Bericht vorzulegen.
3. der IT-Sicherheit höchste Priorität einzuräumen; hierzu gehört, den Einsatz von sogenannten Backdoors zu verurteilen und eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen.
4. von der Geheimhaltung von IT-Sicherheitslücken abzusehen und ein ein Schwachstellen-Management für den Umgang mit IT-Sicherheitslücken einzurichten, das vorsieht, dass alle staatlichen Stellen verpflichtet sind, IT-Sicherheitslücken, von denen sie Kenntnis erlangen, dem BSI zu melden und das marktübliche Verfahren (responsible disclosure) anzuwenden, welches das Verfahren nachvollziehbar dokumentiert, ausreichenden Sachverstand einbezieht und einen jährlichen Bericht der Bundesregierung an den Deutschen Bundestag über den Umgang mit Schwachstellen vorsieht.
5. nicht die absehbare Entscheidung des Europäischen Gerichtshofes zu den deutschen Regelungen zur Vorratsdatenspeicherung abzuwarten, sondern diese Regelungen aufzuheben und als Alternative eine begrenzte anlassbezogene Speicherpflicht auf richterliche Anordnung hin (sog. „Quick-Freeze"-Verfahren) einzuführen, bei dem lediglich Daten eingefroren werden, die ohnehin anfallen, um auch Polizei und Strafverfolgungsbehörden ein praktikables und verfassungsrechtlich zulässiges Ermittlungsinstrument an die Hand zu geben.
6. die Regelungen zu den grundrechtlich aufgrund ihrer Eingriffsintensität höchst problematischen Maßnahmen der Quellen-Telekommunikationsüberwachung und Online-Durchsuchung in der Strafprozessordnung an die Vorgaben des Bundesverfassungsgerichts anzupassen, insbesondere die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sowie die Eingriffsvoraussetzungen, und hierbei beide Maßnahmen einheitlich den Voraussetzungen der Online-Durchsuchung den gleichen Voraussetzungen zu unterwerfen, da sie beide heimlich die Integrität von IT-Systemen verletzten, damit - potentiell - den Zugriff auf das gesamte IT-System ermöglichen und eine verlässliche Grenzziehung technisch wie praktisch nicht möglich ist.
7. ein Musterpolizeigesetz zu erarbeiten, um den Bundesländern eine rechtsstaatliche Orientierungshilfe zu geben und die Spirale der immer weitergehenden Verschärfungen der Landespolizeigesetze zu beenden.
8. die Nachrichtendienste nicht mit den Befugnissen zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung auszustatten.
9. eine Föderalismuskommission III einzusetzen, welche Vorschläge zur Neuordnung der Kompetenzen und Verantwortlichkeiten auf dem Feld der inneren Sicherheit im Verhältnis zwischen Bund und Ländern entwickelt.
10. sich zum Schutz der Privatsphäre und zur Erhöhung der IT-Sicherheit für ein Recht auf Verschlüsselung und gegen jede Beschränkung kryptographischer Sicherungssysteme einzusetzen sowie Telekommunikations- und Telemedienanbieter zu verpflichten, ihre Dienste zukünftig als Standard abhörsicher (Ende-zu-Ende verschlüsselt) anzubieten, wie bereits im Antrag der Fraktion der FDP "Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken" (BT-Drucks. 19/5764) gefordert.

11. den Gestaltungsauftrag zur Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, den das Bundesverfassungsgericht mit der Entwicklung des „IT-Grundrechts“ verbunden hat, endlich ernst zu nehmen und das geltende Recht systematisch zu überprüfen (z.B. die Durchsicht von Datenbeständen, die in der „Cloud“ gespeichert sind, nach § 110 Abs. 3 Strafprozessordnung) und zu ergänzen (z.B. durch die Verpflichtung der Hersteller von Hard- und Software zur Berücksichtigung der Grundsätze des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen (privacy by design and default)).

Berlin, den 15. Oktober 2019

Christian Lindner und Fraktion